Microsoft Digital Identity Update

Thesis

- Web services create inflection point for connected systems
- Growing identity challenges and danger creates increasing friction
  - Organized international identity theft and phraud
  - Password fatigue
  - Privacy concerns
- Removing friction benefits everyone - including Microsoft
- Solving identity problem essential to unleash potential of Web services

What is a digital identity?

- A set of **claims** someone makes about me
- Many identities for many uses
- Required for transactions in real world and online
- Useful to distinguish from **profiles**

Identity is Matched to Context

In Context

- Bank card at ATM
- Gov't ID at border check
- Coffee card at coffee stand
- MSN Passport at HotMail

Out of Context?

- Gov't ID at ATM
- SSN as Student ID
- MSN Passport at eBay

Out of Context

- Coffee card at border check

Lessons from Passport

- Passport designed to solve two problems
  - Identity provider for MSN
    - 250M+ users, 1 billion logons per day
  - Identity provider for the Internet
    - Unsuccessful
- Learning: solution must be different than Passport

The Laws of Identity

An Industry Dialog

1. User control and consent
2. Minimal disclosure for a defined use
3. Justifiable parties
4. Directional identity
5. Pluralism of operators and technologies
6. Human integration
7. Consistent experience across contexts

Join the discussion at www.identityblog.com

The Laws of Identity

An Industry Dialog

1. **User control and consent**
2. **Minimal disclosure for a defined use**
3. **Justifiable parties**
4. **Directional identity**
5. **Pluralism of operators and technologies**
6. **Human integration**
7. **Consistent experience across contexts**

Join the discussion at www.identityblog.com

Lessons from Passport

- Passport designed to solve two problems
  - Identity provider for MSN
    - 250M+ users, 1 billion logons per day
  - Identity provider for the Internet
    - Unsuccessful
- Learning: solution must be different than Passport

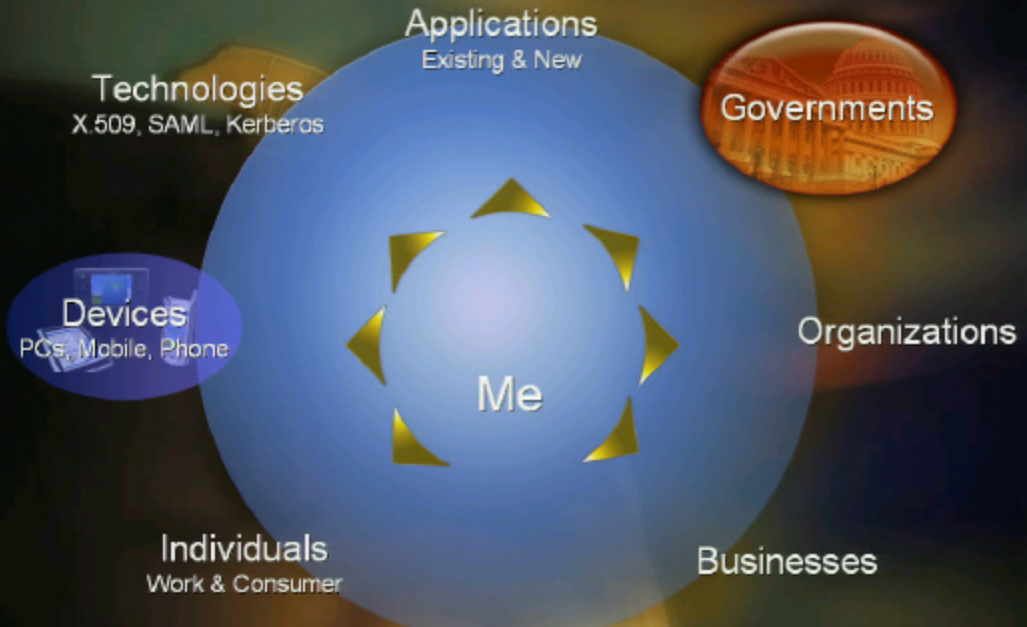
The Laws of Identity

An Industry Dialog

1. User control and consent
2. Minimal disclosure for a defined use
3. Justifiable parties
4. Directional identity
5. Pluralism of operators and technologies
6. Human integration
7. Consistent experience across contexts

Join the discussion at www.identityblog.com

The Laws Define a **Metasystem**



The Laws of Identity

An Industry Dialog

1. User control and consent
2. Minimal disclosure for a defined use
3. Justifiable parties
4. Directional identity
5. Pluralism of operators and technologies
6. Human integration
7. Consistent experience across contexts

Join the discussion at www.identityblog.com

The Laws Define a **Metasystem**

Identity Metasystem

- Consistent way to use multiple identity systems
  - Remove friction without requiring everyone agree on one identity technology for everything
  - Leverage current successes
  - Enable us to move from past to future
- Four key characteristics
  - Negotiation
  - Encapsulating protocol
  - Claims transformation
  - Consistent user experience

Metasystem Players

Identity Providers
Issue identities

Relying Parties
Require identities

Subjects
Individuals and other entities about whom claims are made

Negotiation

- Enable relying party, subject, and identity provider to negotiate
  - Which claims are required
  - Who can make them
  - What type of technology is acceptable
  - Under what conditions claims will be issued
  - How parties prove who they are
  - How information will be used

Encapsulating Protocol

- Technology-agnostic way to exchange policies and claims between Identity Provider and Relying Party
- Content and meaning of what is exchanged determined by participants, not metasystem

Claims Transformation

- Trusted way to change one set of claims into another
  - Specialized server + policy and trust framework for translating foreign claims to locally relevant claims
- Bridge organizational and technical boundaries
  - Transform semantics
    - "Microsoft Employee" -> "Book Purchase OK"
  - Transform formats
    - X.509, SAML1.0, SAML 2.0, SXIP, LID, etc
- Provides interoperability needed today plus flexibility required for future evolution

Consistent User Experience

- Single experience across multiple systems
  - Two-way authentication
  - Uniform logon and registration experience
  - User consent to disclosure of claims
  - Policies exposed and accessible to user
- Reduced cognitive load on user
  - Make identity experience “real” and tangible instead of ad-hoc
  - Predictable - better informed decision making

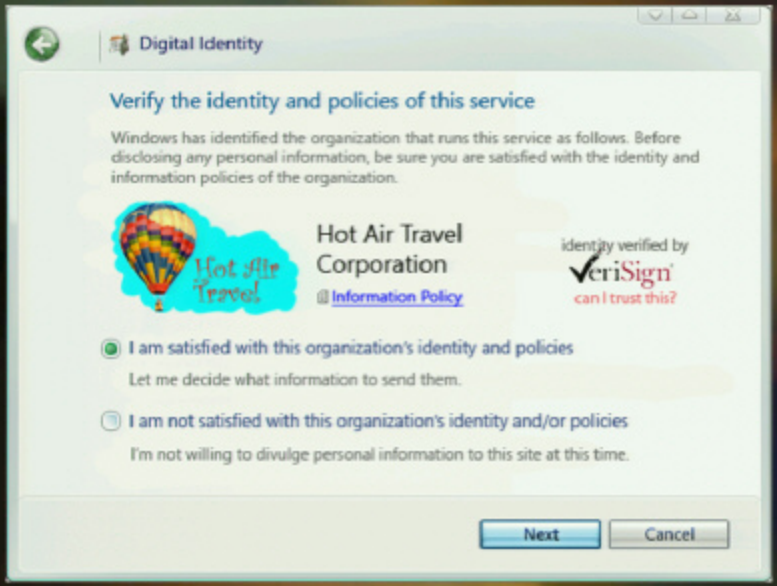
An Identity Metasystem Architecture

- Microsoft worked with industry to develop protocols that enable an identity metasystem: WS-* Web Services
  - Encapsulating protocol and claims transformation: WS-Trust
  - Negotiation: WS-MetadataExchange and WS-SecurityPolicy
- Only technology we know of specifically designed to satisfy requirements of an identity metasystem

Microsoft's Implementation

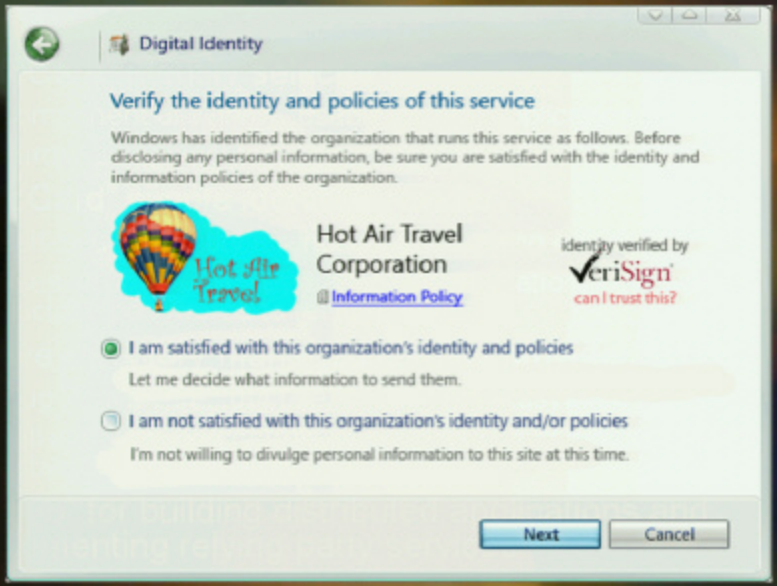
- "InfoCard" identity selector
  - Component of WinFX, usable by any application
  - Hardened against tampering, spoofing
- "InfoCard" simple identity provider
  - Self-issued identity for individuals running on PCs
  - Uses strong public key-based authentication – user does not disclose passwords to relying parties
- Active Directory managed identity provider
  - Plug Active Directory users into the metasystem
  - Full set of policy controls to manage use of simple identities and Active Directory identities
- "Indigo" for building distributed applications and implementing relying party services

Preview – “InfoCard”



Preview – “InfoCard”

Preview – “InfoCard”



WS-* Metasystem Architecture

An Identity Metasystem Architecture

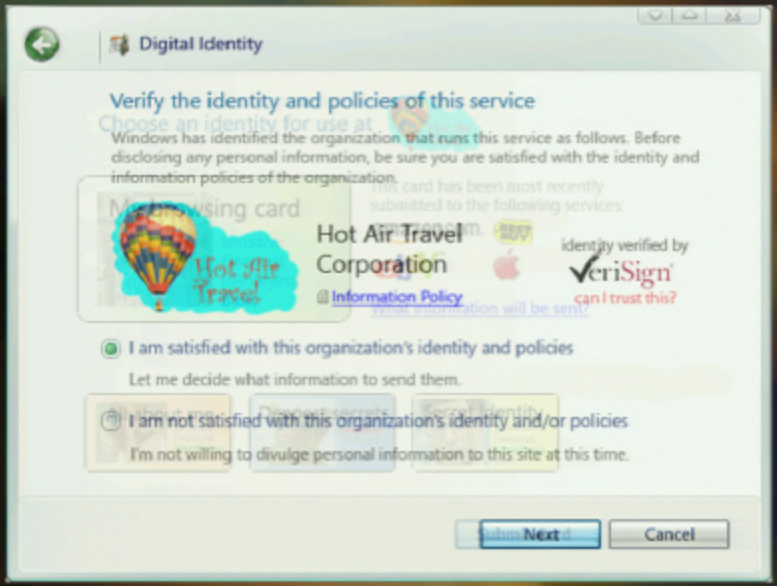
- Microsoft worked with industry to develop protocols that enable an identity metasystem: WS-* Web Services
  - Encapsulating protocol and claims transformation: WS-Trust
  - Negotiation: WS-MetadataExchange and WS-SecurityPolicy
- Only technology we know of specifically designed to satisfy requirements of an identity metasystem

WS-* Metasystem Architecture

Microsoft's Implementation

- "InfoCard" identity selector
  - Component of WinFX, usable by any application
  - Hardened against tampering, spoofing
- "InfoCard" simple identity provider
  - Self-issued identity for individuals running on PCs
  - Uses strong public key-based authentication – user does not disclose passwords to relying parties
- Active Directory managed identity provider
  - Plug Active Directory users into the metasystem
  - Full set of policy controls to manage use of simple identities and Active Directory identities
- "Indigo" for building distributed applications and implementing relying party services

Preview – “InfoCard”



Microsoft's Implementation

- Data stored for each card in card collection
  - Name, logo, names of claims available (not values)
  - Address of identity provider, required credential
- Data stored in simple identity provider
  - Name, address, email, telephone, age, gender
  - User must opt-in
- InfoCard data not visible to applications
  - Stored in files encrypted under system key
  - User interface runs on separate desktop
- Managed identity provider may store information needed to generate claims

Microsoft's Implementation

- Fully interoperable via published protocols
  - With other identity selector implementations
  - With other relying party implementations
  - With other identity provider implementations
- Detailed implementation guide available

Summary

- Laws of Identity define an identity metasystem
- WS-* makes possible an identity metasystem using widely-accepted published protocols
- Microsoft implementing full support for an open identity metasystem in Windows
- Microsoft not launching Son of Passport

- *Identity metasystem has potential to remove friction, accelerate growth of connectivity*
- *Let the identity big bang begin!*

Microsoft's Implementation

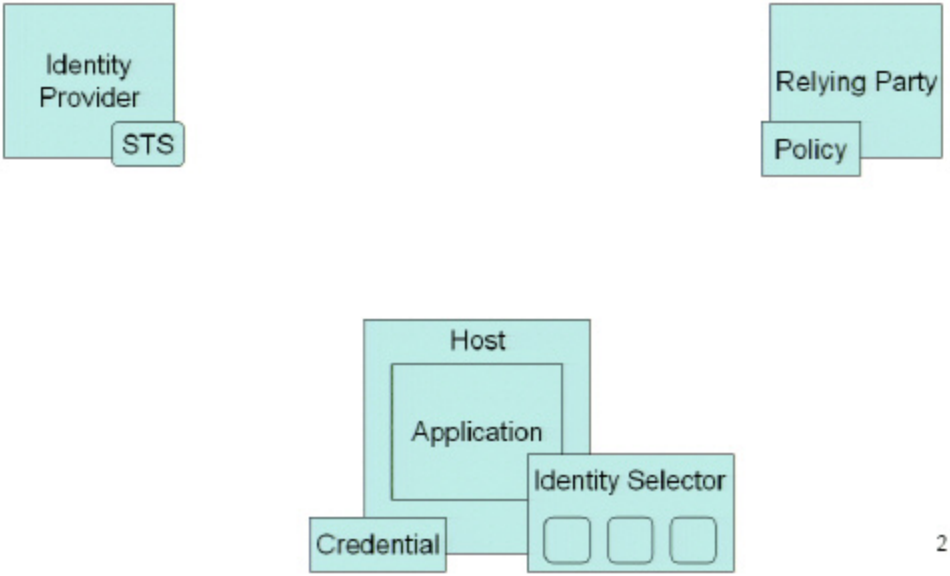
- Data stored for each card in card collection
  - Name, logo, names of claims available (not values)
  - Address of identity provider, required credential
- Data stored in simple identity provider
  - Name, address, email, telephone, age, gender
  - User must opt-in
- InfoCard data not visible to applications
  - Stored in files encrypted under system key
  - User interface runs on separate desktop
- Managed identity provider may store information needed to generate claims

Preview – “InfoCard”

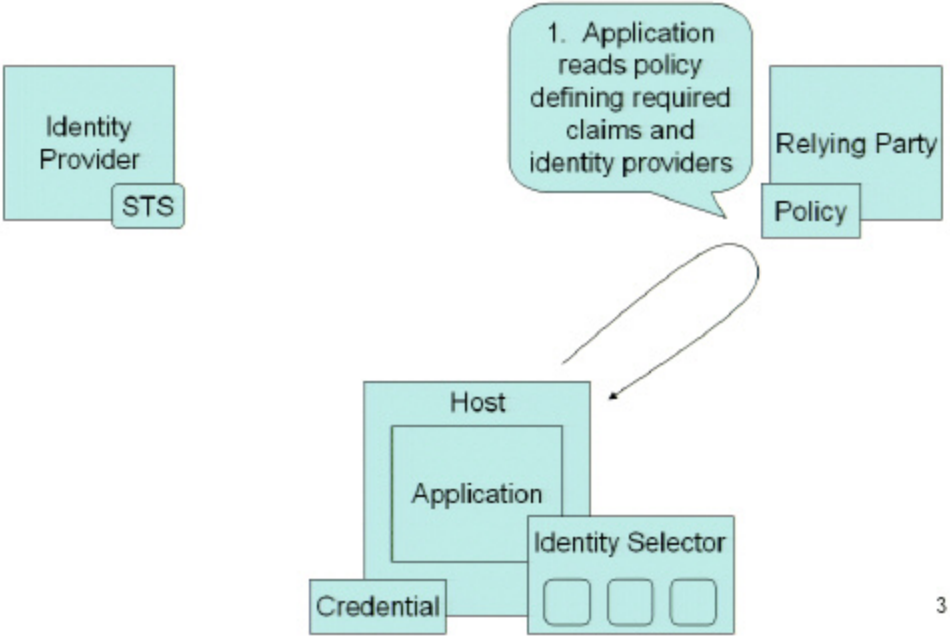
Microsoft Implementation of an Identity Metasystem using WS-*

InfoCard Team

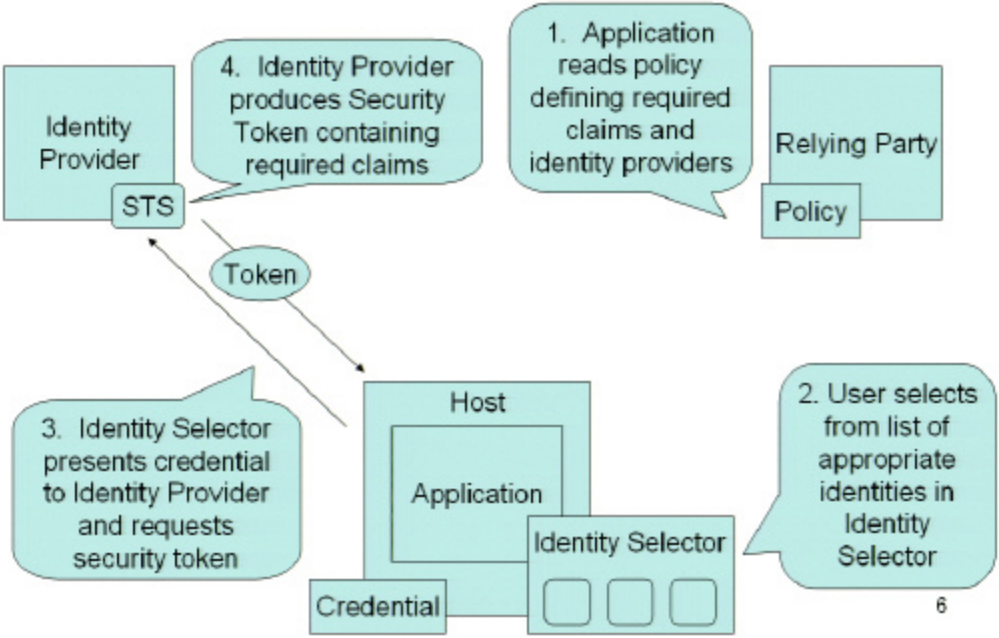
How It Works


Identity Provider
STS
Relying Party
Policy
Host
Application
Identity Selector
Credential

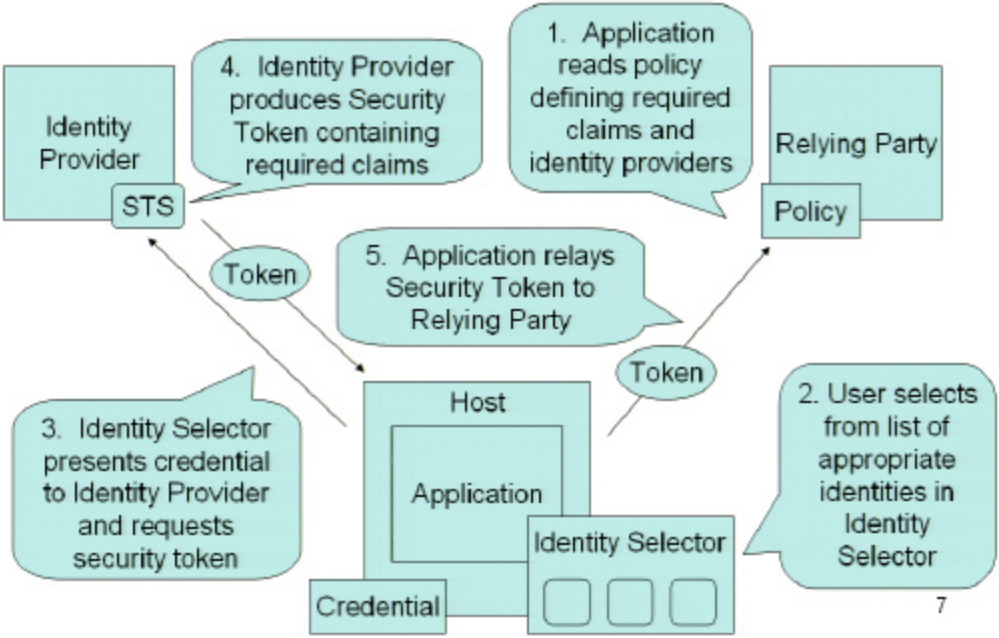
How It Works


Identity Provider
STS
1. Application reads policy defining required claims and identity providers
Relying Party
Policy
Host
Application
Identity Selector
Credential

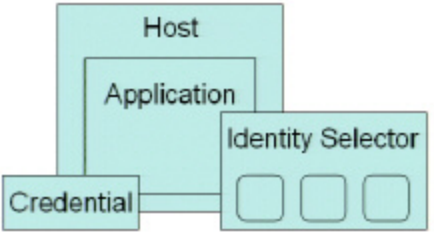
How It Works


1. Application reads policy defining required claims and identity providers
Relying Party
Policy
4. Identity Provider produces Security Token containing required claims
Identity Provider
STS
Token
3. Identity Selector presents credential to Identity Provider and requests security token
Host
Application
Identity Selector
Credential
2. User selects from list of appropriate identities in Identity Selector

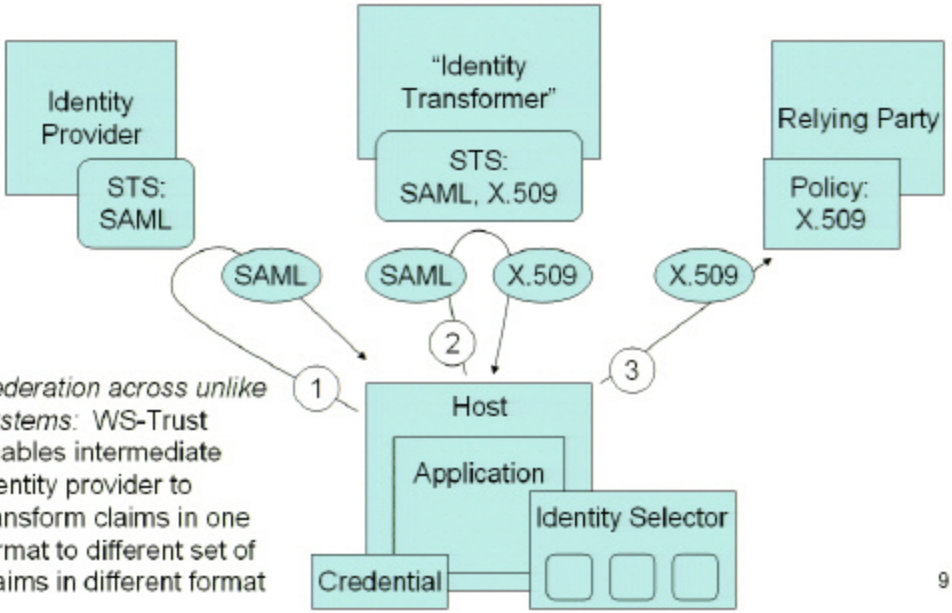
How It Works


Identity Provider
STS
4. Identity Provider produces Security Token containing required claims
1. Application reads policy defining required claims and identity providers
Relying Party
Policy
Token
5. Application relays Security Token to Relying Party
Token
3. Identity Selector presents credential to Identity Provider and requests security token
Host
Application
Identity Selector
Credential
2. User selects from list of appropriate identities in Identity Selector

Claims Transformation



Claims Transformation



Federation across unlike systems: WS-Trust enables intermediate identity provider to transform claims in one format to different set of claims in different format

Identity Selector

- User interface representation of identities
  - Consistent and predictable experience across Identity Providers and Relying Parties
  - Must be safe and trusted
- Show identities available for use at Relying Party
- Show verified identity of Relying Party
  - Facilitate 2-way authentication
- Show use policy of Relying Party
- User consents to disclosure of claims

UX Prototypes

Microsoft Internet Explorer

http://www.amazon.com

Type to Search

File Edit View Favorites Tools Help

Search Favorites

amazon.com | Your Store | See All 31 Product Categories | Your Account | Cart | Wish List | Help

Gift Certificates | International | New Releases | Top Sellers | Today's Deals | Sell Your Stuff

Search Amazon.com GO | Web Search GO

Hello. Sign in to get personalized recommendations. New customer? Start here.

BROWSE

Add Favorites

Featured Stores
- Apparel & Accessories
- Beauty
- DVD's TV Central
- Electronics
- Jewelry & Watches
- Shoes

New Stores
In Beta (What's this?)
- Musical Instruments
- Gourmet Food
- Health & Personal Care
- Sports & Outdoors
- Yellow Pages

Books, Music, DVD
- Books
- DVD
- Magazine Subscriptions
- Music
- Video

Electronics & Office
- Electronics
- Audio & Video

Oprah's Book Club® Is Back!

Oprah just announced her big summer collection--*A Summer of Faulkner*. Oprah's love of the classics continues with this three-book collection of William Faulkner's early works.

For (

Start Again

Join Amazon Prime™

- **Free Two-Day Shipping** or **$3.99-per-item Overnight Shipping** on over a million eligible items sold by Amazon.com
- Ship to any eligible address in the contiguous U.S.
- **Unlimited** privileges cost just $79 per year
- Share these benefits with up to four family members in your household

Learn more and sign up

Penny Shipping on Hot Grills

Ready for Big Trouble?

The Grundig FR200 is ready for emergencies. Crank the handle for AM/FM and shortwave radio or even a flashlight--no power needed for Grundig.

NEW RELEASES

Already a customer? Sign in to see your **New Releases**.

Done

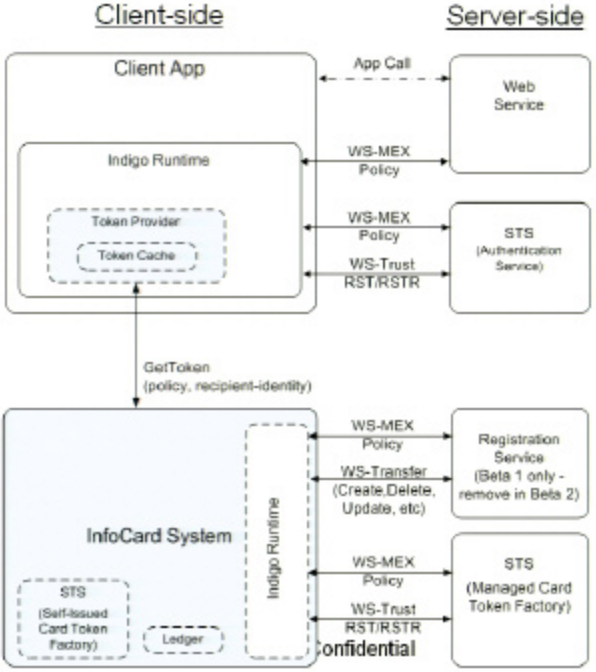
Internet

Done

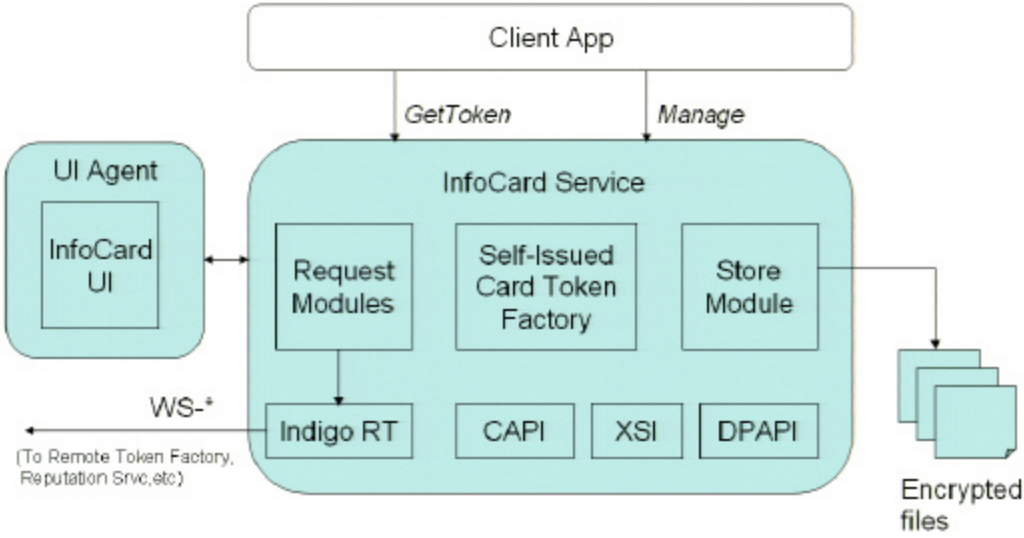
Internet

UX Prototypes

“InfoCard” Architecture Overview

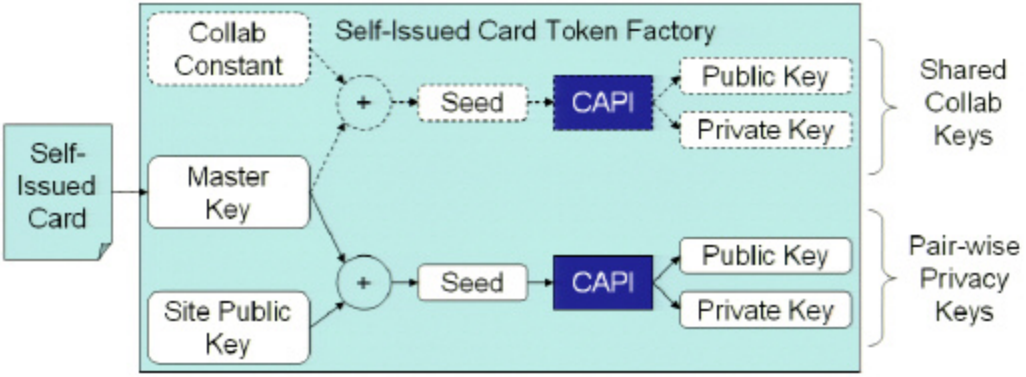


“InfoCard” Protected Subsystem



Curved boxes represent process boundaries

Self-Issued Card Key Generation



- Master key per card
  - Unique pair-wise key derived for each site (no tracking possible)
  - Unique shared key derived for collab (e.g. P2P)
- Easy to roam
  - Only need to roam master key once to each PC
  - Per-site pair-wise keys can be computed dynamically

Roaming Scenarios

- Ad-hoc roaming to trusted computers
  - Manual import/export using removal storage
  - Master keys only need to be roamed once
- Ledger is not roamed

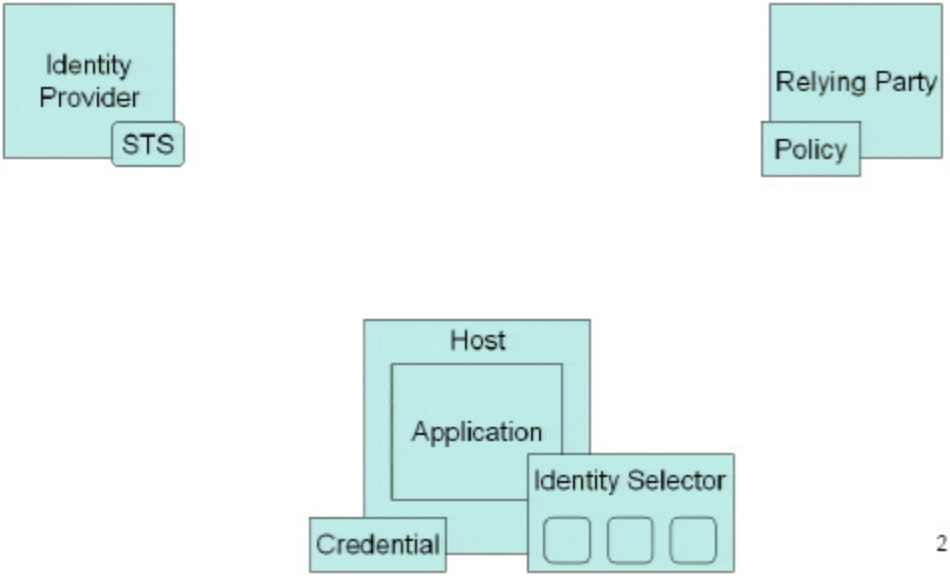
- Future
  - Roam using “Portable STS”
  - Roam using “Vault” in the cloud
  - Dynamic ledger rebuilding

Questions?

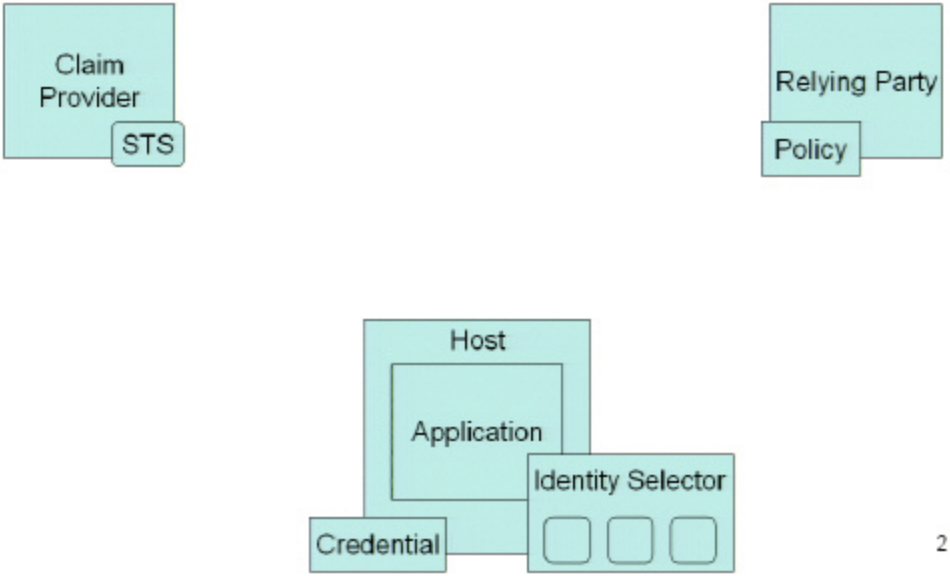
Microsoft Implementation of an Identity Metasystem using WS-*

InfoCard Team

How It Works


Identity Provider
STS
Relying Party
Policy
Host
Application
Identity Selector
Credential

How It Works


Claim Provider
STS
Relying Party
Policy
Host
Application
Identity Selector
Credential